IRON MOUNTAIN®

DATA PROTECTION AND PRIVACY DAY

An opportunity to plan and manage the impact of legal change

Dr. Ross Federgreen, CIPM, CIPP/ US, CIPP/ G, CIPP/ E, CIPP/ C, Fellow, European Privacy Association

DATA PROTECTION AND PRIVACY DAY

Many will know that the stock symbol for Iron Mountain is IRM. They are probably less likely to know that in a different context the acronym IRM stands for Information Rights Management, a term used to describe technologies developed to protect sensitive information - typically documents and emails - from unauthorized access.And many will be unaware of just how important and complex the issue of controlling access to information has become. As Forrester (Nov 2014) recently put it "...in the battle to win, serve and retain customers, data security and privacy have become competitive differentiators..."

In this brief overview of the key concepts of Information Rights Management, we will identify some of the "need to knows" in the field. Simply stated, no organisation, regardless of its size, will remain successful without a comprehensive understanding of the challenges of data lifecycle management and an awareness of the consequences of getting it wrong.

LEGAL FOCUS

The focus of the annual Data Protection Day (DPD), or Data Privacy Day as it's known in North America, is to raise the awareness of individuals and organizations as to their rights and legal obligations when it comes to the collection, storage and distribution of personal data. Iron Mountain strongly believes in the issues of data governance. One of the company's core values is security and it supports the dissemination of important information for the purposes of education, guidance and understanding of what constitutes best practice in information governance.

DPD is celebrated on January 28th because the date corresponds with the 1981 opening for signature of the Council of Europe's Convention 108 for the protection of individuals with regard to the automatic processing of personal data. For over 30 years, European governments and many others worldwide have viewed the privacy of personal data as a fundamental human right. This is consistent with the 1948 United Nations' Universal Declaration of Human Rights.

PERSONALLY IDENTIFIABLE INFORMATION

Over 100 sovereign nations have enacted laws to regulate the use of personal data which is known today as Personally Identifiable Information (PII). Individual rights vary based on where an individual resides, declares citizenship or conducts commerce.

The definition and application of PII continues to expand. Information can be identified or de-identified. De-identified information is material that has been modified so that the owner or individual reflected therein can no longer be identified. However, the effectiveness of de-identification has become more problematic as various programs have been designed to re-identify the de-identified material. Furthermore, as the vast stores of big data available for commercial and governmental utilization continue to expand, the mantra for many has become collect all, store all, save all and ultimately analyse all.

Another concept which is now being applied is that of harmonisation. Many geopolitical zones such as the European Union, APAC and others are attempting to place their privacy laws in a consistent continuum for ease of application and enforcement.

European Union General Data Protection Regulation (GDPR)

The pending European Union General Data Protection Regulation (GDPR) will become a major law with global impact. It is set to replace the 1995 Data Protection Directive known as EU Directive 95-46-EU. The 1995 Directive has served the European community well for 20 years but has become outdated as a consequence of advances in technology, judicial rulings and intellectual thought. It is important to note from a legal view point that the GDPR, being a regulation, carries much stronger legal requirements than the 95 directive: the regulation is a mandate, whereas the directive was guidance. It is imperative to understand that essentially organizations everywhere, both within and external to the European Union, will be impacted by the GDPR.

The GDPR has not been finalised to date (January, 2015) and will have to clear several additional legislative hurdles before becoming law within the EU. It is expected that the European Council will continue to work at a technical level through the second quarter of 2015. Negotiation on the proposed text between the Council and the European Parliament will start when the Council is ready. In early 2016, agreement between the various parties on the draft is expected and then the revised finalized Data Protection framework is expected to come into force in 2018.

There are a number of key concepts and definitions within the GDPR that must be understood in detail as they are embedded in the final framework and underpin the legal and ethical rationale. Further, the obvious and not so obvious economic consequences and burdens

In early 2016, agreement between the various parties on the GDPR draft is expected and then the revised finalized Data Protection framework will come into force in 2018.

of these requirements are far reaching and have not as yet been fully defined. These economic burdens may, in fact, shift the balance as to whether or not any entity should collect PII in the first place.

Data subject and personal data

The first key concept to understand is the definition of data subject and personal data. Data subjects are people who can be directly or indirectly identified from their data either by the data controller, defined as the person or persons who determine the purposes for which and the manner in which any personal data are processed, and or by a third party using reasonably likely means. Personal data refers to all data relating to a data subject.

Legitimate interest pursued by a controller

The second important concept is legitimate interest pursued by a controller (Article 6(1) (f)). This is one of six grounds for the lawfulness of processing. It is important to understand that the legitimate interest of the data controller does not override the fundamental rights and interests of the data subject, especially when the data subject is a child. The five other grounds for the lawfulness of processing are: consent, the need to perform a task in the public interest, the need to fulfil a contract, a legal obligation, and the data is necessary to the vital interests of the data subject.

Consent

A third key concept is "consent". This is defined as freely given, specific and explicit indication of wishes either by statement or by clear affirmative action. Consent, however, is not a legal basis for data processing if there is significant imbalance of power between the controller and the data subject, such as between an employee and the employer.

Portability

A fourth key concept, data portability, has two operational considerations. First, if data is processed in an electronic format, data subjects should be able to obtain a copy of the data in a format that allows them to use it further (Article 18(1)). Second, if data is processed based on consent or contract, data subjects should be able to take the data they have supplied with them when changing service providers (Article 18 (2)).

The right to be forgotten

Our fifth key concept, "the right to erasure or the right to be forgotten", has already sparked much controversy and discussion. There are two specific actions that are important here. First, when the data controller has no reason to further process data, or when the data has been processed in breach of the Regulation, the data subject is entitled to have the data deleted (Article (17(1)). The data subject must submit a request asking the data controller to delete the data. Second, where the controller has already made the personal data public, the controller must then take all reasonable steps to inform third parties who are processing the data of the request to delete any links to or copies of the personal data (Article 17 (2)).

Data breach notification

The final key concept we address here is, "data breach notification". Data breach notification is the obligation to provide information quickly when information has been compromised as a consequence of malicious intent or inadvertent disclosure. Article 31 requires data controllers to notify their supervisory authorities without undue delay and where feasible within 24 hours of discovery of a breach. Article 32 requires the notification of data subjects where there is the possibility of adverse effect without delay. The standard that must be met is that of "likely to affect". Again this standard has not been rigidly defined or litigated to date.

We have not addressed many of the other significant issues and consequences of failure to meet the requirements of the GDPR within this short discussion. Such items as the requirements for a Data Protection Officer (DPO) and the fines which can be levied must again be understood and where appropriate complied with.

CONCLUSION

In summary, the GDPR will become the law for data in the European Union and it is our strong belief that this will extend globally. We are using today – Data Protection Day – to help you prepare for what is ahead. It's essential that organisations in every geography gain a detailed working knowledge of how it will affect their day to day operations, and the significant economic consequences for failure to do so.

Iron Mountain is committed to keeping you informed of the progress of enactment of the GDPR and of the actions you will need to take to respond.

IRON MOUNTAIN®

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks, and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.co.uk for more information.